AFFIDAVIT OF SPECIAL AGENT KELLY M. BELL IN SUPPORT OF CRIMINAL COMPLAINT AND APPLICATIONS FOR SEARCH WARRANTS

I, Kelly M. Bell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent for the Federal Bureau of Investigation ("FBI") currently assigned to the Boston, Massachusetts Field Office. I have been employed as a Special Agent for more than fifteen years. I am currently tasked with the investigation of economic crimes, and my previous experience includes investigations of wire fraud, bank fraud, money laundering, bankruptcy fraud, and mortgage fraud. I have received on-the-job training as well as participated in FBI-sponsored training courses on these types of investigations. My investigations and training have included the use of surveillance techniques and the execution of search, seizure, and arrest warrants.

2. I am currently investigating FELIX GOROVODSKY ("GOROVODSKY") for various crimes, including but not limited to: bank fraud, in violation of Title 18, United States Code, Section 1344; aggravated identity theft, in violation of Title 18, United States Code, Section 1028A; wire fraud, in violation of Title 18, United States Code, Section 1343; and money laundering, in violation of Title 18, United States Code, Section 1957.

3. I submit this affidavit in support of a criminal complaint charging GOROVODSKY with bank fraud, in violation of Title 18, United States Code, Section 1344. As set forth below, I have probable cause to believe that from in and around March 2019 through at least May 2020, GOROVODSKY executed a scheme to defraud Capital One Bank USA, N.A. ("Capital One") by stealing retirement savings that an elderly victim ("VICTIM-1") kept in the custody and control of Capital One.

4. Specifically, I have probable cause to believe that as part of the scheme, GOROVODSKY, who had previously secured a power of attorney from VICTIM-1 before she revoked it, fraudulently accessed one of VICTIM-1's Capital One bank accounts and transferred more than $250,000 of VICTIM-1's retirement savings to GOROVODSKY's personal checking account. GOROVODSKY used those stolen retirement savings for personal expenses, including paying off more than $100,000 in federal student loans. As a further part of the scheme, when Capital One began an investigation, GOROVODSKY forged VICTIM-1's signature on a purported "gift letter," and then sent the forged gift letter to Capital One in an attempt to legitimize his fraudulent transfer and evade detection of the fraud. Accordingly, and as further set forth below, I have probable cause to believe that GOROVODSKY knowingly and willfully executed a scheme and artifice to obtain money under the custody or control of a financial institution, by means of materially false or fraudulent pretenses, representations, and promises, and by concealment of material facts, in violation of Title 18, United States Code, Section 1344.

5. I also submit this affidavit in support of an application for a warrant under Title 18, United States Code, Section 2703(a) and Federal Rule of Criminal Procedure 41 to search and seize records and data from two e-mail accounts, as further identified in Attachment A-1 and pursuant to the procedures detailed in Attachment B-1: (1) Gorovodsky@gmail.com ("Target Account 1"); and (2) Mkamburova1937@gmail.com ("Target Account 2," and collectively with Target Account 1, the "Target Accounts"). Based on the domain names of the Target Accounts, I have probable cause to believe that the Target Accounts and relevant data are maintained by Google LLC ("Google"), which government databases indicate accepts service of process via web portal at USLawEnforcement@google.com, as further described in Attachment A-1.

6. I also submit this affidavit in support of an application for a warrant to search the residence of GOROVODSKY at 18 Paradise Road, Swampscott, Massachusetts 01907 (the "Subject Premises"), as further described in Attachment A-2, because there is probable cause to believe that it contains evidence, fruits, and instrumentalities of the crimes listed above, as further described in Attachment B-2. As set forth below, there is probable cause to believe that evidence, fruits, and instrumentalities of GOROVODSKY's fraud scheme will be found where he resides, including on his computer and cellular phone.

7. The facts in this affidavit come from my participation in this investigation, including my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. In submitting this affidavit, I have not included every fact known to me about this investigation. Rather, I have included only those facts that I believe are sufficient to establish probable cause for: (1) the criminal complaint charging GOROVODSKY with bank fraud, in violation of Title 18, United States Code, Section 1344; (2) the warrant for the Target Accounts; and (3) the warrant for the Subject Premises.

PROBABLE CAUSE

A. Certain Relevant Persons and Entities

8. GOROVODSKY, age 29, is a resident of Swampscott, Massachusetts. From in or about June 2018 until February 2020, GOROVODSKY lived in Singapore, where he worked as an information technology project manager for INTERPOL and ran his own information technology consulting business. GOROVODSKY speaks Russian.

9. In 2014, GOROVODSKY obtained a bachelor's degree from a college in Massachusetts. In 2016, GOROVODSKY obtained a master's degree in information technology from a graduate school in Massachusetts, and in 2018, GOROVODSKY obtained a master's in

business administration from the same graduate school. GOROVODSKY financed his education, in part, with student loans. In or about April 2020, GOROVODSKY had more than $100,000 in outstanding federal student loans.

10. VICTIM-1 was born in Russia in 1942. In or about 1988, VICTIM-1 and her husband immigrated to the United States, where they purchased a home in Houston, Texas.

11. On or about October 10, 2006, VICTIM-1 and her husband prepared and signed their last will and testament. VICTIM-1 and her husband each left their estates in their entirety to their surviving spouse, and in the event both of them died, to a Houston church where they were longtime parishioners.

12. In or about 2017, after VICTIM-1 and her husband had initiated plans to sell their Houston home and retire to Ecuador, VICTIM-1's husband died. In or about 2018, VICTIM-1 moved to Salinas, Ecuador, where she presently resides. VICTIM-1 has never traveled to Singapore.

13. Capital One is a financial institution that is a member of the Federal Deposit Insurance Corporation ("FDIC"). Capital One is headquartered in McLean, Virginia.

B. Background of the Fraud Scheme

14. In or about November 2018, VICTIM-1 began seeking an advisor to assist her in managing her finances and retirement assets, including the proceeds from the anticipated sale of her Houston home. VICTIM-1 sought an advisor who spoke Russian.

15. In or about December 2018, a relative of GOROVODSKY referred GOROVODSKY to VICTIM-1 as a potential financial manager and advisor.

16. On or about December 15, 2018, VICTIM-1 appointed GOROVODSKY as her financial proxy and hired him as a financial manager and advisor for a monthly fee, after

GOROVODSKY touted his investing experience to VICTIM-1. In reality, GOROVODSKY had no significant professional experience or accreditations in investing or finance.

17. Using his personal e-mail address, Target Account 1, GOROVODSKY sent VICTIM-1 invoices for the management and advisory services that he performed, and VICTIM-1 paid GOROVODSKY for those services. For example, on or about March 26, 2019, GOROVODSKY sent VICTIM-1 an invoice for approximately $1,120, which included a base monthly fee, as well as fees for researching stock investments. On or about March 29, 2019, VICTIM-1 paid GOROVODSKY for his services by transferring approximately $1,120 from her checking account to a checking account in GOROVODSKY's name.

18. As part of his duties as VICTIM-1's financial manager and advisor, GOROVODSKY also collected VICTIM-1's bank and credit card statements, and from Target Account 1, sent them to her on a monthly basis. For example, on or about May 12, 2019, GOROVODSKY sent VICTIM-1 her credit card statement, writing in Russian: "statements only from March to April. Not ready from April to May."[1]

C. The Fraud Scheme

19. As set forth in further detail below, beginning at least in or around March 2019, GOROVODSKY began executing a scheme to defraud Capital One, and VICTIM-1, by stealing retirement assets that VICTIM-1 maintained in the custody and control of Capital One, specifically, the proceeds from the sale of VICTIM-1's home in Houston. In or about April 2020, GOROVODSKY accessed VICTIM-1's Capital One bank accounts without her knowledge or authorization, and fraudulently transferred approximately $252,915 to his own Capital One checking account. GOROVODSKY then used that money for personal purposes,

[1] References herein to statements in Russian are based on draft translations.

including to pay off his federal student loans and credit card debt. As a further part of the scheme, GOROVODSKY forged VICTIM-1's signature on a sham "gift letter" that he sent to Capital One in an attempt to substantiate the fraudulent transfer, and he falsely told Capital One that VICTIM-1's signature on the forged gift letter had been witnessed by a notary public.

The Sale of VICTIM-1's Home

20. In or about March 2019, VICTIM-1 decided to sell her Houston home and sought GOROVODSKY's advice in investing the proceeds to support her during her retirement. On or about March 2, 2019, VICTIM-1's Houston home was listed for sale.

21. On or about April 9, 2019, Target Account 2, an e-mail account in VICTIM-1's name, was created without her knowledge or consent. A review of records shows that Target Account 2 was created using an internet protocol ("IP") address[2] in Singapore (where GOROVODSKY was working in April 2019), and that Target Account 1 (GOROVODSKY's personal e-mail address) and Target Account 2 share the same internet cookies.[3]

22. On or about April 20, 2019, VICTIM-1's home in Houston went under contract, and the sale was pending.

23. On or about the same day, April 20, 2019, GOROVODSKY advised VICTIM-1, who had been a longtime client of a different bank, to open a money market account with Capital One, where GOROVODSKY had an existing checking account with an account number ending in -7575 (the "7575 Account").

[2] An IP address is a unique numerical identifier assigned to every machine on the internet. *See United States v. McLellan*, 792 F.3d 200, 204 n.1 (1st Cir. 2015).

[3] An internet cookie is a piece of data that stores user web preferences, as well as login and registration information. *See In re Pharmatrak, Inc.*, 329 F.3d 9, 14 (1st Cir. 2003) (describing cookies).

24. On or about April 20, 2019, at GOROVODSKY's behest, VICTIM-1 opened a Capital One money market account with an account number ending in -0548 (the "Money Market Account"). GOROVODSKY assisted VICTIM-1 in opening the account. Later that same day, from a Singapore IP address, the Money Market Account was enrolled in Capital One online banking, and GOROVODSKY was added as a joint account holder without VICTIM-1's authorization. The confirmation e-mail for the addition of GOROVODSKY as a joint account holder was sent to Target Account 2, which was the e-mail account created in VICTIM-1's name without her knowledge from a Singapore IP address.

25. On or about April 24, 2019, the mailing address for the Money Market Account was changed to the Subject Premises in Swampscott, Massachusetts. The address change was executed via a Singapore IP address. As detailed further below, the Subject Premises is a home owned by a trust that lists GOROVODSKY and a relative of GOROVODSKY as trustees.

26. On or about April 30, 2019, Capital One issued the first monthly bank statement for the Money Market Account. Although the monthly statement listed VICTIM-1's name, the address listed was the Subject Premises in Swampscott, Massachusetts, and the e-mail address listed was Target Account 2.

27. On or about April 30, 2019, the sale of VICTIM-1's home in Houston was finalized, pending closing.

The Power of Attorney

28. One day later, on or about May 1, 2019, GOROVODSKY began making arrangements to meet VICTIM-1 in Houston so that he could assist her in investing the forthcoming proceeds from the sale of her home. On or about May 1, 2019, GOROVODSKY used his American Express credit card ending in -1008 to purchase tickets for VICTIM-1 to fly

from Ecuador to Houston, and he sent the tickets to VICTIM-1 from Target Account 1, his personal e-mail address.

29. On or about May 9, 2019, approximately $266,970.41 in proceeds from the sale of VICTIM-1's Houston home was deposited by the title company into the Money Market Account.

30. On or about May 15, 2019, GOROVODSKY and VICTIM-1 met in Houston, with GOROVODSKY traveling from Singapore and VICTIM-1 traveling from Ecuador. GOROVODSKY provided VICTIM-1 with his business card, which listed a cellular phone number of 617-818-3037. GOROVODSKY drove VICTIM-1 to an attorney in Houston. The attorney drafted a document granting GOROVODSKY power of attorney for VICTIM-1.

31. The power of attorney provided that GOROVODSKY would act as a fiduciary for VICTIM-1. VICTIM-1 signed the power of attorney, and her signature was notarized by a notary public in Houston.

32. Based on interviews and a review of records, VICTIM-1 did not sign any additional documents on May 15, 2019 that granted GOROVODSKY further rights, gifts, or benefits. No additional documents were presented to the notary public who witnessed and notarized VICTIM-1's signature on the power of attorney.

33. Later the same day, on or about May 15, 2019, at GOROVODSKY's behest, VICTIM-1 opened an interest-bearing Capital One certificate of deposit account ending in -0376 (the "CD Account"), and she transferred approximately $250,000 from the Money Market Account to the CD Account.

34. On or about the following day, May 16, 2019, GOROVODSKY was added as a joint account holder to the CD Account without VICTIM-1's authorization, and the confirmation of that addition was e-mailed to Target Account 2.

The Power of Attorney Revocation

35. After VICTIM-1 returned to Ecuador on or about May 18, 2019, she decided that she no longer wanted GOROVODSKY to hold power of attorney or to serve as her financial manager and advisor.

36. On or about July 8, 2019, VICTIM-1 traveled from Ecuador to Houston, accompanied by a friend, in order to revoke GOROVODSKY's power of attorney and terminate his role as her financial advisor.

37. On or about July 9, 2019, VICTIM-1 traveled to the office of a different Houston attorney. The attorney drafted a revocation of power of attorney that stated: "This instrument revokes the Power of Attorney appointing Felix GOROVODSKY as my agent and attorney-in-fact executed by [VICTIM-1] on May 15, 2019. All provisions of the Statutory Durable Power of Attorney with regard to any of my property, including any and all bank accounts and accounts at financial institutions wherever located are null and void, abandoned, terminated and revoked. This revocation is effective immediately."

38. VICTIM-1 signed the revocation of power of attorney, and her signature on the revocation was notarized by a notary public.

39. A copy of the notarized revocation was sent to GOROVODSKY from the attorney's office, by both mail and e-mail. The revocation was accompanied by a cover letter to GOROVODSKY that informed him: "Please be advised that effective July 9, 2019, you are no

longer authorized to act as [an] agent on behalf of [VICTIM-1] as her Statutory Durable Power of Attorney has been revoked."

The Liquidation of VICTIM-1's Bank Account

40. On or about March 8, 2020, GOROVODSKY traveled from Singapore to Boston and began living at the Subject Premises in Swampscott, Massachusetts.

41. On or about March 23, 2020, GOROVODSKY applied to the United States Department of Education for borrower forgiveness for certain student loans. As of that date, GOROVODSKY had more than $100,000 in federal student loans, and he was behind on payments for those loans.

42. On or about April 1, 2020, GOROVODSKY had a balance of $0 in the 7575 Account (his personal Capital One checking account), and approximately $26.41 in his Capital One savings account ending in -0342 (the "0342 Account"). GOROVODSKY also had at least $13,000 in credit card debt.

43. On or about April 9, 2020—nine months after VICTIM-1 revoked the power of attorney and terminated GOROVODSKY as her financial advisor—GOROVODSKY signed into his Capital One online banking account, and without VICTIM-1's knowledge or consent, transferred approximately $252,915.98 from her CD Account to his personal checking account. GOROVODSKY used the remaining funds in the CD Account to pay an early withdrawal penalty of approximately $3,399.22.

44. GOROVODSKY immediately began to spend the transferred funds on personal expenses. On or about April 9, 2020, GOROVODSKY transferred approximately $40,000 from the 7575 Account to the 0342 Account (his personal Capital One savings account), and then used the funds to pay off more than $23,000 in credit card debt and charges during April 2020. Also

on or about April 9, 2020, GOROVODSKY withdrew approximately $101,266.46 from the 7575 Account and used that money to pay off his federal Department of Education student loans. During April 2020, GOROVODSKY also withdrew more than $14,000 of the stolen funds via ATMs in and around Swampscott, Massachusetts, his Venmo account, and his brokerage account.

The Forged "Gift Letter" and Lies to Capital One

45. On or about May 2, 2020, Capital One froze the remaining $93,371.85 in the 7575 Account and the 0342 Account.[4]

46. On or about May 4, 2020, in response to an inquiry from Capital One, GOROVODSKY e-mailed Capital One from Target Account 1, his personal e-mail address, attaching a "Notice/Letter of Gifting" that purportedly bore VICTIM-1's signature and was dated May 15, 2019—the same date of the power of attorney that VICTIM-1 subsequently revoked. The "gift letter" that GOROVODSKY sent to Capital One was not notarized.

47. GOROVODSKY advised Capital One as follows (all *sic* in original): "After searching through my files I have found the Notice/Letter of Gifting. That [VICTIM-1] had signed on May 15th 2019. This letter was signed in front of a Notary Republic. I only kept the attached file for records. [VICTIM-1] does have the signed copy with a Notary Stamp in her files. . . . Again, attached outside of the Notice/Letter of Gifting I've attached the Power of Attorney that I have."

[4] On or about November 13, 2020, Capital One filed an interpleader action in the United States District Court for the Southern District of Texas concerning the $93,371.85 frozen in the 7575 and 0342 Accounts, plus an additional $17,100.11 in frozen funds remaining in the Money Market Account. *See Capital One, N.A. v. Gorovodsky*, Case No. 4:20-cv-03864 (S.D. Tex.).

48. The purported "gift letter" that GOROVODSKY sent to Capital One states (all *sic* in original): "This Notice/Letter of Gifting is written proof to a verbal agreement I made to Felix Gorovodsky. That I [VICTIM-1] have opened a Joint Bank Account Capital One 360 Money Market CD with Felix Gorovodsky. This account was opened and funded as a gift to Felix Gorovodsky to help pay off his Student Loans and provide him with a living stipend as I do not bear any children or immediate family. The 360 Money Market CD account # ([]-0376) opened on May 14, 2019, with both names. As of May 14, 2019, Felix, has the right to close this account before its Maturity, to access the funds."

49. The signature on the "gift letter" that GOROVODSKY sent to Capital One appears to be a digital copy of VICTIM-1's signature on the May 15, 2019 power of attorney.

50. In his May 4, 2020 e-mail from Target Account 1 to Capital One attaching the forged "gift letter," GOROVODSKY did not notify Capital One that VICTIM-1 had revoked the power of attorney.

51. Based on interviews that I have conducted and my review of records, VICTIM-1 did not sign the "gift letter," and did not make any verbal agreement to give GOROVODSKY her retirement assets as a "gift."

TARGET ACCOUNTS – PROBABLE CAUSE TO BELIEVE THAT THE ACCOUNTS CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES

52. I have probable cause to believe that the Target Accounts and associated data contain evidence, fruits, and instrumentalities of the crimes identified above.

53. As set forth in further detail above, Target Account 1—GOROVODSKY's personal e-mail account Gorovodsky@gmail.com—is the account that GOROVODSKY used to communicate with VICTIM-1. Further, GOROVODSKY used Target Account 1 to

communicate with Capital One, including to send Capital One the forged "gift letter" and the false statement that VICTIM-1 possessed a signed, notarized copy of the "gift letter."

54. As set forth in further detail above, Target Account 2—Mkamburova1937@gmail.com—is the e-mail address that was created, from Singapore, in VICTIM-1's name without her knowledge and that received confirmation e-mails from Capital One regarding the changes to VICTIM-1's accounts, such as the addition of GOROVODSKY as a joint account holder. Further, a review of records indicates that Target Account 2 shares internet cookies with GOROVODSKY's personal e-mail address.

55. On or about December 4, 2020, Assistant United States Attorney Ian Stearns sent Google a letter requesting under 18 U.S.C. § 2703(f) that the company preserve records associated with the Target Accounts for 90 days.

TARGET ACCOUNTS – TECHNICAL BACKGROUND

56. Google user-generated data is preserved indefinitely, unless the user deletes it or opts into an autodelete schedule. IP addresses and login logs are held by Google for approximately 180 days.

57. E-mail providers also typically maintain electronic records relating to their customers. These records include account application information, account access information, and e-mail transaction information.

58. Google can also provide the following additional information associated with a subscriber's account: address book information; location history; search and browsing history; photos; files; and data.

TARGET ACCOUNTS – LEGAL AUTHORITY

59. The government may obtain both electronic communications and subscriber information from an e-mail provider by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

60. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the website hosting company or e-mail provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

61. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

62. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this Court, regardless of where Google has chosen to store such information. Pursuant to 18 U.S.C. § 2713, the government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

TARGET ACCOUNTS – FOURTEEN-DAY RULE FOR EXECUTION OF WARRANT

63. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the

Court issues this warrant, the United States will execute it not by entering the premises of Google, as with a conventional warrant, but rather by serving a copy of the warrant on the company and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

64. Based on my training and experience and my understanding from other law enforcement agents, I understand that e-mail providers sometimes produce data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that e-mail providers sometimes produce data that was created after this 14-day deadline ("late-created data").

65. The United States does not ask for this extra data or participate in its production.

66. Should Google produce late-created data in response to this warrant, I request permission to view all late-created data that was created by Google, including subscriber, IP address, logging, and other transactional data, without further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

67. For these reasons, I request that the Court approve the procedures in Attachment B-1, which set forth these limitations.

SUBJECT PREMISES – PROBABLE CAUSE TO BELIEVE THE SUBJECT PREMISES CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES

68. As set forth in further detail above, and as summarized below, I also have probable cause to believe that the Subject Premises to be searched contains fruits, evidence, and instrumentalities of violations of the federal statutes listed above, as described in Attachments A-2 and B-2.

69. A review of records indicates that in April 2020—the month of the transfer from VICTIM-1's CD Account to the 7575 Account owned by GOROVODSKY—the mailing address for both the CD Account and the 7575 Account was the Subject Premises.

70. On or about April 9, 2020, GOROVODSKY used the funds transferred into the 7575 Account, in part, to pay off credit card debt. A review of records indicates that in April 2020, the mailing address for that credit card was the Subject Premises.

71. On or about December 4, 2020, GOROVODSKY signed into Target Account 1, his personal e-mail address from which he sent Capital One the forged "gift letter", via a Comcast IP address ending in -1be9. A review of records indicates that as of that date, that IP address was assigned to Comcast high-speed internet subscriber FELIX GOROVODSKY, with a service and billing address at the Subject Premises, and a contact phone number of GOROVODSKY's cellular phone, 617-818-3037. As of January 11, 2021, the account status was "active" for GOROVODSKY's high-speed internet subscription at the Subject Premises.

72. From December 21, 2020 through January 15, 2021, the FBI conducted surveillance at the Subject Premises on several occasions. On each occasion, a grey Chevy Silverado bearing Massachusetts license plate number 1TWR28 was parked in the immediate vicinity of the Subject Premises (as is visible from one of the photographs in Attachment A-2).

Public database checks identify GOROVODSKY as the owner of the Chevy Silverado, which is financed by a loan from Citizens Bank to GOROVODSKY.

73. Public database checks identify the owner of the Subject Premises as F & Y Realty Trust. In 2014, GOROVODSKY's mother and GOROVODSKY created F & Y Realty Trust, naming themselves as trustees. On the same day, GOROVODSKY's mother granted quitclaim deed for the Subject Premises to herself and GOROVODSKY, as trustees for F & Y Realty Trust.

74. The Subject Premises, 18 Paradise Road, is comprised of the second and third floors of a duplex home. 16 Paradise Road (a two-bedroom, one-bathroom apartment) is located on the first floor of the duplex home. Both the Subject Premises and 16 Paradise Road have entrances at the front of the home, with the front entrance to the Subject Premises on the right and the front entrance to 16 Paradise Road on the left. As of January 18, 2021, the apartment at 16 Paradise Road was publicly listed for rent, with GOROVODSKY listed as the property owner, and a contact phone number of GOROVODSKY's cellular phone number, 617-818-3037.

SUBJECT PREMISES – SEIZURE OF COMPUTER EQUIPMENT AND DATA

75. There is probable cause to believe that electronic equipment was used to violate federal law, and that the equipment will be found at the Subject Premises set forth in Attachment A-2.

a. From my training and experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching

topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

b. Further, based on my training, experience, and information provided by other law enforcement officers, I know that many cellular phones (which are included in Attachment B-2's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device.

c. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B-2 in computer hardware, computer software, smartphones, and storage media.

d. A review of records indicates that on or about April 9, 2020—the same day that GOROVODSKY liquidated VICTIM-1's CD Account, transferring $252,915.98 to his personal checking account—GOROVODSKY signed into Capital One online banking through a computer web login via a Massachusetts IP address.

e. A review of records also indicates that on or about the same day, April 9, 2020, GOROVODSKY signed into Capital One online banking through a mobile login on an Apple iPhone via the same Massachusetts IP address.

f. Further, a review of records indicates that on or about May 4, 2020—the same day that GOROVODSKY sent the forged "gift letter" from Target Account 1 to Capital One—GOROVODSKY signed into Target Account 1 via a Massachusetts IP address.

g. As set forth above, a review of records indicates that on or about December 4, 2020, GOROVODSKY signed into Target Account 1 via a Comcast IP address that is assigned to GOROVODSKY as the subscriber for Comcast high-speed internet at the Subject Premises.

76. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media in particular, computers' internal hard drives contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the

chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

77. Based on my knowledge, training, and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence that storage media, such as hard disks, flash drives, CDs, and DVDs, can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

c. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

78. The premises may contain computer equipment whose use in the crime or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B-2 are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

79. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B-2 because they are associated with GOROVODSKY. For example, the agents will attempt to identify the cellular phone belonging to GOROVODSKY by calling his cellular phone number during the search, 617-818-3037. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, or if it appears that GOROVODSKY has more than one cellular phone and/or computer, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

80. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied or disclosed

pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

SUBJECT PREMISES – UNLOCKING DEVICE USING BIOMETRIC FEATURES

81. As discussed above, a review of records indicates that it is likely that the Subject Premises will contain at least one Apple iPhone (or other mobile device) belonging to GOROVODSKY.

82. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellular phones made by Apple and other manufacturers, offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

83. For example, on the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked; and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been

entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if: (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

84. The passcode that would unlock the Apple iPhone or other device found during the search of the Subject Premises is not currently known to law enforcement. Thus, it may be useful to press the finger(s) of the user(s) of to the device's fingerprint sensor or to hold the device up to the face of the owner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

85. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it may be necessary for law enforcement to have the ability to require any occupant of the Subject Premises to press their finger(s) against the sensor of the locked device(s) or place the devices in front of their faces in order to attempt to identify the device's user(s) and unlock the device(s).

86. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the Subject Premises to the sensor of the devices or place the devices in front of their faces for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

87. Based on my knowledge, training and experience, and the facts as set forth in this affidavit, I have probable cause to believe and I do believe that GOROVODSKY committed bank fraud, in violation of Title 18, United States Code, Section 1344.

88. Further, based on the information above, I also have probable cause to believe that records and data from the Target Accounts (as described in Attachment A-1) contain evidence, fruits, and instrumentalities of the above-listed crimes (as described in Attachment B-1). The procedures for copying and reviewing these records are set forth in Attachment B-1.

89. Further, based on the information above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B-2, are contained within the Subject Premises described in Attachment A-2.

Respectfully submitted,

Kelly M Bell

Kelly M. Bell, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me telephonically on January 21, 2021.

Jennifer C. Boal

The Honorable Jennifer C. Boal
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS